CJDY

AO 91 (REV.5/85) Criminal Complaint

AUSA Benjamin F. Langner (312) 353-2817

FILED

OCT 11 2011

OCT 11 2011

MICHAEL W. DOBBINS
CLERK, U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA

v.

YIHAO PU,
also known as "Ben Pu"

CRIMINAL COMPLAINT

CASE NUMBER: 11CR0699

UNDER SEAL

MAGISTRATE JUDGE VALDEZ

I, the undersigned complainant, being duly sworn on oath, state that the following is true and correct to the best of my knowledge and belief: On or about August 22, 2011, at Chicago, in the Northern District of Illinois, Eastern Division YIHAO PU, also known as "Ben Pu," defendant herein:

> with the intent to convert trade secrets that are related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending that the offense will injure any owner of the trade secrets, without proper authorization copied, duplicated, downloaded, uploaded, replicated, transmitted, sent and conveyed trade secrets, namely File 1, File 2 and File 3 which contained trade secrets belonging to Citadel, LLC, and attempted to do so;

in violation of Title 18, United States Code, Section 1832. I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the facts contained in the Affidavit which is attached hereto and incorporated herein.

Signature of Complainant
ROBERT L. WALKER
Special Agent, Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

October 11, 2011 at Chicago, Illinois
Date City and State

MARIA VALDEZ, U.S. Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

UNITED STATES DISTRICT COURT)
) ss
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, ROBERT L. WALKER, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation, and have been so employed for 20 years. My current responsibilities include the investigation of white collar crime, including mail, wire, and bank fraud.

2. This affidavit is submitted in support of a criminal complaint alleging that Yihao Pu, also known as Ben Pu, has violated Title 18, United States Code, Section 1832. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging PU with theft of trade secrets, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the defendant committed the offense alleged in the complaint.

3. This affidavit is based on my personal knowledge, information provided to me by other law enforcement agents and interviews of witnesses, as set forth below.

FACTS SUPPORTING PROBABLE CAUSE

I. Citadel, LLC, and its Trade Secrets

4. According to Jonathan Graham—Managing Director of Citadel, LLC—Citadel is a financial firm whose businesses include investments and technology-related products and

services. According to Graham, Citadel is a Delaware limited liability company with its principal place of business in Chicago and investors located in Illinois and elsewhere.

5. According to Graham, one of Citadel's businesses, referred to as Tactical Trading ("TT"), deploys automated electronic trading strategies to identify short-term investment opportunities in global equities, futures, and other investment instruments. More specifically, according to Graham, Citadel's TT employees—many of whom have Ph.Ds in mathematics, physics, and other fields—research and create mathematical and statistical computer models that identify and quantify relationships among investment instruments and market activities. Those relationships are then translated into algorithms and integrated into computer source code for electronic trading programs that automatically execute trading orders upon the occurrence of certain events in the markets.

6. According to Graham, the building blocks of Citadel's TT trading algorithms and strategies are prediction signals, commonly referred to as "alphas," which use incoming market data and other data to predict the movement of investment instruments and other relevant market activity.[1] According to Graham, the output of the alpha algorithms are expressed as numerical values, and are referred to by Citadel employees as "alpha data." According to Graham, the alpha data are unique number sequences that have inherent value as a result of their relationship to the alpha algorithms.

---

[1] Furthermore, according to Graham, the alphas are comprised of smaller data-based computations referred to as alpha "terms."

7. According to Graham, if a company gained access to Citadel's alphas, that company would have a significant advantage in writing the code and strategies to implement a competitive business or to improve an existing competitive business. Furthermore, according to Graham, alpha data could be used by a company to reverse engineer the alphas themselves. According to Graham, if a company—even an individual trading alone—obtains Citadel's alphas and makes trades based on the alphas, those trades would compete with Citadel's trades and could thereby limit or eliminate the profits that Citadel could make using its proprietary trading strategies.

8. According to Graham, Citadel has spent and continues to spend a considerable amount of money developing, testing, maintaining and updating the proprietary information used in Citadel's TT business (collectively, its "Trade Secrets"), which includes but is not limited to its alpha terms, alphas (or signals), alpha data, strategies, statistical models, algorithms and source code.

9. According to Graham, within the past year Citadel has used its Trade Secrets to generate significant profits through trades of various investment products according to the predictions generated by Citadel's alpha trading strategies. According to Graham, Citadel's Trade Secrets generally retain much of their value over time, and the trading strategies researched and developed for use today are likely to generate profits for months and years in the future with only minor modifications and updates to account for market changes.

A. Secrecy of Trade Secrets

10. According to Graham, Citadel has expended, and continues to expend, a considerable amount of money and resources to ensure the secrecy of its Trade Secrets. According to Graham, Citadel does not disclose its Trade Secrets to its investors or any third parties, and employs various security measures to safeguard the secrecy of its Trade Secrets, including but not limited to:

a. restricting access to Citadel's office space to employees and pre-approved visitors through the use of an electronic access card;

b. further restricting access to sensitive areas of Citadel's office space to only those employees who work in a specific portion of Citadel's business;

c. requiring employees to utilize a username, password and privacy tokens to access the computer system;

d. restricting employees' computer access to only those portions of the Trade Secrets on which they need to work;

e. barring employees from encrypting or password-protecting information on their computers without prior company approval;

f. blocking employees from plugging external storage devices into work computers by systematically disabling ports on Citadel computers to prevent copying of Trade Secrets;

g. restricting access to the source code containing the algorithms and the sensitive data such as alpha data to a limited set of Citadel employees;

h. employing security cameras and security guards to monitor its facilities; and

i. aggressively discouraging written (or plain language) summaries of the source code or the mathematical and statistical models and algorithms reflected in the source code.

11. Furthermore, according to Graham, Citadel requires employees to sign non-disclosure agreements related to its Trade Secrets and requires almost every member of the TT business to sign a non-compete agreement.

II. Yihao Pu's Employment with Citadel

12. According to Citadel records, Yihao "Ben" PU was hired by Citadel in May 2010 as a Quantitative Financial Engineer, and worked at Citadel from May 2010 until he was terminated by Citadel on August 30, 2011. According to Citadel records, PU resides at an apartment located in Chicago, Illinois.

13. According to Graham, as a Quantitative Financial Engineer, it was PU's job to work with analysts and researchers to develop and enhance certain of Citadel's proprietary trading strategies. More specifically, according to Graham, PU assisted with the trade/order placement logic, helped to de-bug the trading strategies after they were developed and, in part because of his high-level computer skills, was assigned various computer-based tasks

unconnected to his direct responsibilities. According to Graham, as a result of the work PU was performing for Citadel, PU was permitted to use his office computer to access a folder stored on Citadel's servers that contained information and data related to Citadel's alphas. However, according to Graham, none of PU's assigned tasks involved downloading alpha-related information to external storage devices or making investment trades based on alpha-related information, nor was PU permitted to make use of alpha-related information outside of Citadel for any purpose.

14. According to Citadel's records, on or about March 25, 2010, in connection with his acceptance of a position with Citadel, PU signed and entered into several agreements with Citadel, including a Non-Disclosure Agreement and a Non-Competition Agreement. In the Non-Disclosure Agreement, PU agreed that "I will use Confidential Information only as required to perform my duties for Citadel (and not for my personal benefit or for the benefit of any other individual or entity)." The Non-Disclosure Agreement defines Confidential Information as including "information relating to Citadel's internal financial affairs . . .; strategies; portfolio holdings; . . . portfolio management techniques; quantitative analytics and models used to evaluate financial instruments; proprietary software (including the proprietary system architectures); and [Citadel's] business and investment processes." The Non-Disclosure Agreement further provides that, "I understand that any loss or erosion of Citadel's competitive advantage through the disclosure or improper use of its Confidential

Information could have severe repercussions on Citadel's business, including the possibility of substantial investment losses for [Citadel and its clients]."

15. According to Graham and as noted above, in order to protect the security of its Trade Secrets, Citadel programmed the computers they distributed to employees—including the computer they provided to PU in order for PU to perform his duties as assigned by Citadel—not to recognize electronic storage devices, such as external hard drives or thumb drives, if such devices were plugged into the ports of the computer.

III. Yihao Pu's Theft of Citadel's Trade Secrets

16. Chris Herringshaw—an Information Technology Professional employed by Citadel—reported that on August 25, 2011, an employee in Citadel's IT department noticed that PU had an unusually large quantity of data and programs associated with his user profile on Citadel's computer systems, and Citadel initiated an investigation of PU's computer activities. According to Herringshaw, Citadel's IT staff discovered that PU had configured and was running two virtual computers—a sub-divided space on the hard drive operating as its own hard drive, also referred to as "virtual machines"—on his Citadel computer, with each virtual machine residing on PU's computer's hard drive.[2]

---

[2] The IT staff also discovered that PU had downloaded a "port scanner" program to his Citadel computer which, according to Herringshaw, is a tool commonly used by hackers to locate weakness in computer networks and which can also be used to locate data or files on multiple servers. According to Herringshaw and Graham, port scanner software is neither required, nor helpful, to the type of work that PU was hired to perform for Citadel. Furthermore, according to Herringshaw, the IT staff discovered that PU had improperly downloaded a "Bit Torrent" program, which allows users to rapidly upload and download files, in violation of Citadel's IT and security policies.

17. According to Herringshaw, the IT staff further discovered that PU had downloaded and used Ubuntu Linux, an open-source computer operating system, to run the virtual machines on his Citadel computer, and had encrypted and password-protected the data contained on at least one of the virtual machines. According to Herringshaw, the creation of virtual machines and installation of Ubuntu Linux to run those machines allowed PU to bypass Citadel's security protocols and transfer files or data from his Citadel computer to an external storage device. According to Herringshaw, neither the existence of this virtual machine nor the password securing the virtual machine had been disclosed to Citadel by PU.

A. Yihao Pu Is Confronted by Citadel and Turns Over Certain Storage Devices to Citadel

18. According to Herringshaw, on August 26, 2011, at about 10:30 a.m., Herringshaw and several other Citadel employees and attorneys confronted PU concerning the virtual machines on his work computer. In response, according to Herringshaw, PU admitted to Herringshaw and others that he had uploaded files from his Citadel computer, but claimed to have only uploaded information onto one external device, his Droid mobile phone. According to Herringshaw, PU also insisted that he had uploaded only academic papers and music files from his Citadel computer to his mobile phone.

19. According to Herringshaw, at the conclusion of the interview, Michael Weiner, Citadel's in-house counsel, requested that PU preserve all of his personal computers and electronic storage devices because the computers and devices were relevant evidence in Citadel's investigation, and PU replied "I understand."

20. According to Weiner, in the early afternoon of August 26, 2011, after PU had left Citadel's office, Weiner called PU and asked PU to return to the office so that Citadel could copy the files on PU's Droid phone. According to Weiner, PU agreed to return to Citadel's offices.

21. According to Weiner, PU returned to Citadel's office at about 5:30 p.m. and allowed a technician from FTI Consulting—a computer forensic company hired by Citadel—to copy the files on his Motorola Droid cellular telephone (hereafter the "Motorola Droid Phone"). According to Weiner, while in Citadel's offices, PU also gave a Western Digital 500 GB external hard drive (hereafter the "Western Digital Hard Drive"), to Weiner and the FTI technician, and told Weiner that he (PU) had copied some "market data" onto the Western Digital Hard Drive, but had already deleted the market data prior to bringing the hard drive to Citadel.

B. PU Attempts to Destroy Evidence

22. Individual A—a friend of PU who has known PU since approximately November 2010 and who was interviewed by the government pursuant to a proffer agreement—told investigating agents that he talked to PU by phone around noon on Friday, August 26, 2011, and PU asked Individual A to come to PU's apartment, but would not explain on the phone why he needed Individual A to come over. According to Individual A, when he arrived at PU's apartment, Individual B was already inside PU's apartment and

shortly thereafter Individual C, a mutual friend who worked with PU at Citadel, arrived at PU's apartment.

23. Individual A told investigating agents that when he asked PU how he was doing, PU told Individual A that PU might go to jail. According to Individual A, PU told Individual A that Citadel wanted PU to turn over all of his computers to Citadel. According to Individual A, PU told Individual A that PU intended to "hide" some of his computer equipment from Citadel. According to Individual A, there were several computers in PU's apartment and while he was there, PU took the hard drive out of several of the computers.

24. According to Individual A, later that afternoon, he drove PU to Citadel's offices and PU went inside. Individual A went to dinner with Individual C and Individual D, and then Individual A and Individual C met with PU at PU's apartment later that evening. According to Individual A, at around 11:00 p.m., PU asked Individual A and Individual C to help carry computer equipment out to Individual A's car. Individual A told agents that Individual A, Individual C and PU carried a desktop computer, monitors and bags containing hard drives and other computer peripherals to Individual A's car. According to Individual A, PU asked Individual A to take the computer equipment to Individual A's apartment and said that he [PU] would come over later and set up the computer equipment. Individual A told agents that he drove the computer equipment to his residence and left the computer equipment in the car overnight.

25. According to Individual A, on Saturday, August 27, 2011, in the late morning or early afternoon, PU came over the Individual A's apartment and Individual A helped PU carry the computer equipment up to Individual A's apartment. Individual A told agents that, once inside the apartment, PU set up and started operating the computer equipment, telling Individual A that he was "cleaning" the hard drives.[3] According to Individual A, when PU was finished around 4:00 p.m., PU went back to Citadel's offices but left the computer equipment in Individual A's apartment.[4]

26. According to Individual A, on Sunday, August 28, 2011, in the morning, Individual A sent a text message to PU asking PU whether Individual A could put the computer equipment at someone else's house or whether he should give the hard drives back to PU. According to Individual A, PU called him back and told him, in Chinese, "don't be stupid" and instructed him to stop sending text messages about the computer equipment. PU later explained to Individual A that PU did not want Citadel to know that PU owned more hard drives than the ones that PU had turned over to Citadel.

---

[3] Based on my training and experience, I understand "cleaning" a hard drive to refer to measures taken to eliminate data or information (and traces thereof) that had previously been stored on an electronic device.

[4] According to Weiner, he again called PU in the afternoon of Saturday, August 27, 2011, and during the ensuing conversation, PU admitted to Weiner that after the meeting between PU and various Citadel employees and attorneys on Friday morning, PU had "scuttled" a hard drive onto which PU had copied files from his Citadel work computer. According to Herringshaw, shortly after the phone call between Weiner and PU, Herringshaw called PU to discuss the scuttled hard drive and PU told Herringshaw that PU had encrypted the external hard drive and destroyed all copies of the encryption key, thereby preventing anyone, even himself, from accessing the hard drive.

27. According to Individual A, later that afternoon, PU came over to Individual A's apartment, turned on the computer equipment and worked further on cleaning the computer hard drives. According to Individual A, after PU was finished with the computer, PU and Individual A went to a CVS store and PU purchased two disposable phones, gave one of the phones to Individual A, gave Individual A the phone number to the other disposable phone and told Individual A to call him on the disposable phone.

28. According to Individual A, at approximately 9:00 p.m. on Sunday, August 28, 2011, PU called Individual A and told Individual A to "just dump everything." Individual A told investigating agents that PU further explained that Individual A should dump the computer equipment into a dumpster so that a garbage truck would pick it up. According to Individual A, PU told Individual A not to throw away the most important hard drive—which PU had earlier identified for Individual A—and to keep that hard drive for PU to pick up at a later time (the Seagate Hard Drive, *see* ¶¶ 30-31).

29. According to Individual A, after the phone call with PU, he drove north from his apartment looking for a place to dump the computer equipment and, after stopping several times to dispose of the equipment but changing his mind as to the place and method of disposal, Individual A proceeded to the southeast corner of the intersection of Sheridan Road and the sanitary canal near the Wilmette Harbor. According to Individual A, after walking down several steps to get closer to the water, he threw a shopping bag containing the hard drives given to him by PU over a fence and into the canal. According to Individual A,

Individual A did not throw away the other computer equipment provided to him by PU, including the hard drive that PU indicated was the most important hard drive.

C. Individual A turns over Seagate Hard Drive to Citadel

30. According to Individual A, on August 30, 2011, he gave the hard drive that PU indicated was the most important hard drive to the office manager for Individual A's attorney. According to an Associate Director at Navigant Consulting, Inc., on September 1, 2011, the office manager gave to Navigant a Seagate 2 TB external hard drive (the Seagate Hard Drive), which the office manager indicated was the hard drive he received from Individual A. On September 29, 2011, an agreed order was entered in a civil case pending between Citadel and PU which authorized Citadel to access and review the materials contained on the Seagate Hard Drive.

D. Recovery of Hitachi Hard Drive from Canal

31. According to Dan Roffman, Director of FTI, on September 1, 2011, Roffman, Individual A and others went to the intersection of Sheridan Road and the canal leading to Wilmette Harbor and Individual A showed Roffman and others where he threw the computer equipment he received from PU into the canal.

32. According to Roffman, on September 2, 2011, Roffman observed as a diver retained by FTI entered the canal leading to the Wilmette Harbor and recovered six hard drives from the water in the same location where Individual A indicated he threw the computer equipment. When the diver brought the hard drives to the shore, Roffman

catalogued the hard drives, including a Hitachi 1 TB external hard drive (hereafter the "Hitachi Hard Drive").

E. Preliminary Results of Forensic Investigation

33. According to Roffman, FTI performed a forensic analysis on multiple electronic storage devices connected to this case, including: (a) the Western Digital Hard Drive, (b) the Motorola Droid Phone, (c) Seagate Hard Drive, and (d) Hitachi Hard Drive.[5]

34. According to Roffman, FTI's analysis of the Western Digital Hard Drive revealed that thousands of files had been stored on the hard drive in a folder named "CP2" but had been deleted prior to FTI taking possession of the hard drive.[6] FTI was able to retrieve those files from the hard drive, and discovered the following files, among others, that had been saved in the CP2 folder: (a) File 1, (b) File 2 and (c) File 3 (collectively the "Western Digital Files"). According to Graham, who reviewed the files after they were recovered by Roffman, the Western Digital Files contain certain of Citadel's alpha terms and alpha data. According to Graham, PU had not been assigned to work on a number of the alpha terms and alpha data contained in the Western Digital Files, and therefore had no legitimate reason to ever have accessed and possessed that information.

---

[5] According to Roffman, FTI's analysis of the electronic storage devices is ongoing and FTI may discover additional evidence during the course of that analysis.

[6] According to Roffman, a folder named CP2 had been created on one of the virtual machines located on PU's work computer and the size of the folder as recorded by PU's work computer matched the size of the folder as recorded by the Western Digital 500 GB external hard drive.

35. According to Roffman, FTI's analysis of a Dell Precision computer with serial number 3F379F1, identified by Herringshaw as PU's work computer, revealed that on August 22, 2011, the Western Digital Hard Drive was mounted on the two virtual machines created on the hard drive of PU's work computer. Furthermore, according to Roffman, based on his analysis of the Western Digital Hard Drive, the Western Digital Files were created—or, more specifically, copied or moved to the Western Digital external hard drive —between August 22 and August 24, 2011.

36. According to Roffman, FTI's analysis of the Motorola Droid Phone revealed that the phone contained File 4. According to Graham, File 4 contained certain of Citadel's alpha data.

37. According to Roffman, FTI's analysis of the Hitachi Hard Drive revealed that the hard drive had previously been connected to a Lenovo X300 computer and also contained two photos of PU's driver's license and various other documents and photos apparently belonging to PU.[7] According to Roffman, the Hitachi Hard Drive also contains the following files, among others: (a) File 5 and (b) File 6 (collectively the "Hitachi Files"). According to Graham, the Hitachi Files contain certain of Citadel's alpha data. Furthermore, according to Graham, one of the files on the Hitachi Hard Drive, which was sent to Graham by Roffman after it was recovered by FTI, contained records of investment trades made by

[7] According to Roffman, on Saturday, August 28, 2011, Roffman went to PU's apartment and with PU's consent took possession of several hard drives and a Lenovo X300 computer. According to Roffman, the Western Digital Hard Drive and a Droid mobile phone had also been connected to the Hitachi Hard Drive.

Citadel and investments held by Citadel.

38. According to Roffman, FTI's analysis of the Seagate Hard Drive revealed that the Seagate Hard Drive contains multiple folders and files, including computer source code, that appear to belong to Company A. Citadel's personnel records indicate that PU worked at Company A prior to accepting employment with Citadel. Furthermore, Roffman told agents that the Seagate Hard Drive had been used to access encrypted files located on a website named www.BenPu.net. According to Roffman—who accessed www.BenPu.net with PU's agreement and with a password provided by PU—BenPu.net contains (among other files) a series of text files, written in the months before PU started working at Citadel and stored in a folder named "thoughts," that appear to outline a plan for PU to obtain "execution data" from a computer network and use it to start a hedge fund in China, including steps such as building a "reverse tunnel" on a computer system, reviewing computer code belonging to Company A, and constructing a trading platform based on the stolen execution data.

IV. Yihao Pu's Attempts to Trade Based on Citadel Alpha Information

39. According to Individual A, on or about August 10, 2011, when Individual A was at PU's residence, he observed data on one of the four computer monitors in PU's apartment and, upon Individual A asking about the nature of the data, PU responded that it was "alpha" data. According to Individual A, PU then attempted to explain to Individual A how PU interpreted the data, but Individual A did not understand PU's explanation.

According to Individual A, PU told Individual A that if PU's company knew what he was doing, PU would get fired. Individual A told agents that on another of the four computer monitors, Individual A observed an Interactive Brokers trading account, which Individual A was familiar with based on Individual A's use of Interactive Brokers' online software in his job. Individual A further told investigating agents that on another occasion, when Individual A was in PU's apartment, PU told Individual A that PU had written a program in the java programming code[8] that automatically executed trades from PU's Interactive Brokers' trading account based on data which PU input into the program.

40. According to records obtained from Interactive Brokers, Yihao B. PU owned a trading account with Interactive Brokers that was opened in or about August 2009. The Interactive Brokers records indicate that from August 2009 to January 2011, PU sporadically traded a variety of investment instruments. Beginning in January 2011, the Interactive Brokers records show that PU started trading in currency futures, although the trading was still sporadic. However, beginning in about early August 2011, the Interactive Brokers records show that PU's trading habits changed dramatically: (a) PU exclusively traded six different types of currency futures contracts and two securities exchange futures contracts; (b) the frequency and volume of PU's trading increased exponentially, such that PU made about 3,000 trades in the month of August and was making trades within minutes or even seconds or a prior trade; and (c) PU consistently traded within a narrow range (*i.e.* never

[8] Based on my training and experience, I understand that Java is the name of a specific computer language that is often used to write computer programs.

buying or selling more than 5 contracts and then clearing the position with a trade shortly thereafter). According to Graham, the group within the TT business where PU worked—the statistical arbitrage fixed income commodities and currency group—worked on trading strategies related to currency futures (as well as other instruments) and traded the six currency futures that PU traded through his Interactive Brokers account. Furthermore, according to Graham, the type of trading that PU's Interactive Brokers account evidences—frequent trading, trading in and out of positions within minutes and trading within a narrow range—is consistent with the type of trading conducted by Citadel's TT business where PU worked. Additionally, the type of trading conducted by PU is only rational if associated with a market data based trading strategy because the rapid changes in investment strategy (buying and selling the same instrument in quick succession) could not be explained by non-market data based indicators (*e.g.* economic trends, financial news), and the fees or commissions associated with such frequent trading are exorbitant if the trades are not reliably profitable.

41. According to Graham, certain files recovered from the Hitachi Hard Drive (recovered by FTI from the Wilmette canal) indicate that PU was attempting to construct a trading strategy similar to the one used by Citadel. According to Graham, contained on the Hitachi Hard Drive was a repository of java code that appeared to be a fully functional automated trading system that: (a) loads a file with the same name as one of the Hitachi Files—which contained alpha data—in order to calculate optimal trading times, (b) uses a

set of numerical identifiers for trading instruments (*e.g.* 3749 for IBM stock, 5172 for Yen futures)[9] that is identical to the identifiers that Citadel arbitrarily assigned to those investment instruments and (c) directed trading orders to an Interactive Brokers trading account with the same account number as PU's account and which referenced a username of SBenPu143.[10]

42. Based on the trading activity in PU's Interactive Brokers account and the automated trading system recovered from the Hitachi external hard drive, it appears that PU was attempting to use the alpha data he stole from Citadel to reverse engineer the algorithms containing Citadel's alphas, and was trading currency futures in his brokerage account with Interactive Brokers in order to test the system that he was creating.

---

[9] These are not the actual random numerical identifiers used by Citadel.

[10] Furthermore, according to Roffman, there were approximately 500 java source code files on the Seagate Hard Drive that appear to be earlier versions of the automated trading system found on the Hitachi Hard Drive.

VI. Conclusion

43. Based on the facts set forth above, there is probable cause to believe that defendant YIHAO PU, also known as "Ben Pu," with the intent to convert a trade secret that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending that the offense will injure any owner of that trade secret, without proper authorization copied, duplicated, downloaded, uploaded, replicated, transmitted, sent and conveyed a trade secret, namely File 1, File 2 and File 3 which contained trade secrets belonging to Citadel, LLC, and attempted to do so, in violation of Title 18, United States Code, Section 1832.

FURTHER AFFIANT SAYETH NOT.

ROBERT L. WALKER
Special Agent, Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me on October 11, 2011.

MARIA VALDEZ
United States Magistrate Judge